Leveraging LANL's D-WAVE 2X for Random Number Generation

Sarah Michalak

Rick Picard

michalak@lanl.gov

April 27, 2017

UNCLASSIFIED

LA-UR-17-23343

The Idea

- The DWAVE QPU produces strings of 0s and 1s
- Can they form the basis of a random number generator?
- With the “zero” problem, each qubit theoretically should take the value 1 with probability 0.50

$$\sum_i h_i \sigma_z^{(i)} + \sum_{i>j} J_{i,j} \sigma_z^{(i)} \sigma_z^{(j)}$$

  - But information from DWAVE suggests this ideal is not met
- Non-random bit strings might be transformed to random bit strings

Characterize Ising Bit Strings

- Based on consultation with DWAVE, run the zero problem on Ising while varying two input parameters:
  - Annealing time: 5, 10, 20 microseconds
  - Readout thermalization: 0, 50, 100 microseconds
  - Other parameters set to default values
    - Programming thermalization set to 1000 microseconds
  - 9 test conditions; 8000 samples; don't run during shim times
    - 8000 samples a value that worked for all test conditions

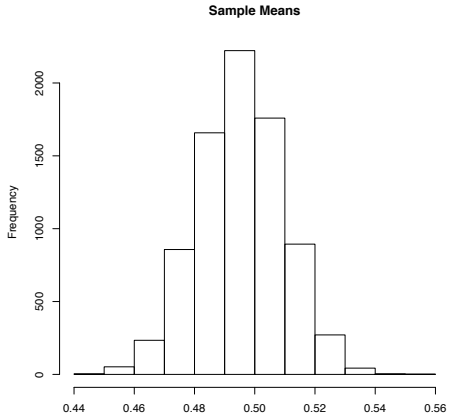
Characterization Strategy

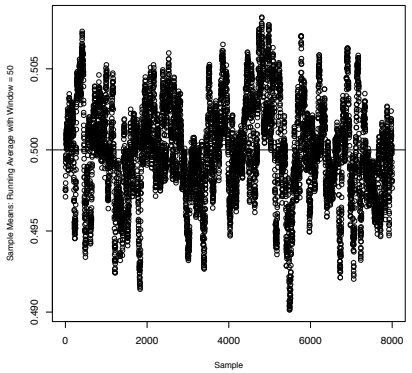
- Consider:
  - Results for each of 8000 samples of 1095 operational qubits
  - Results for each of 1095 operational qubits for 8000 samples
- Characterization includes:
  - Means (probability = 1) (sample and qubit)
  - Spatial (qubit) or temporal correlation* (qubit and sample)

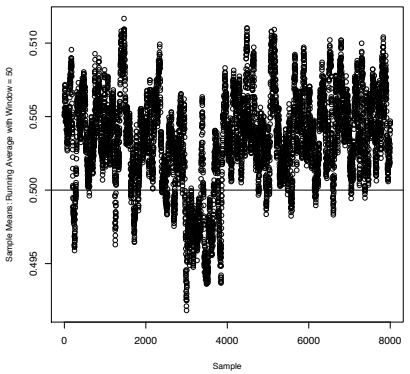
* Although we use the term correlation because of its broad familiarity, association is a better term for binary data.

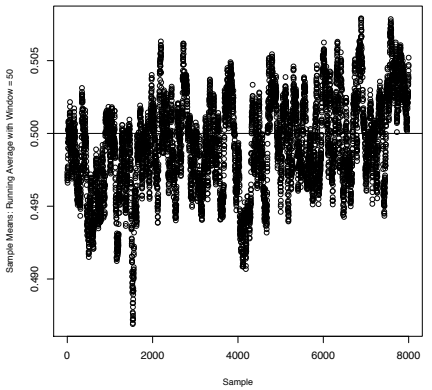
Characterization Results for 8000 Samples

- Mean = mean of 1095 qubit values for each of 8000 samples
  - Vary from about .44 to .56
  - Autocorrelation in sample means



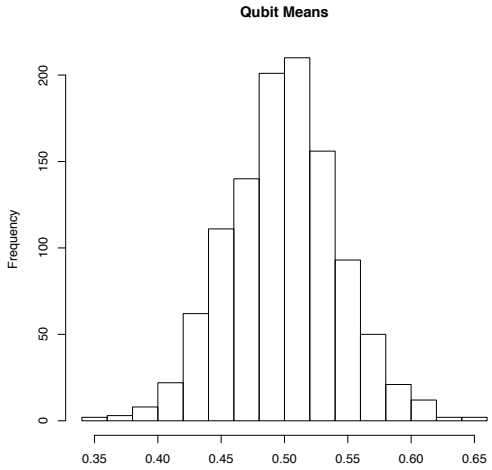


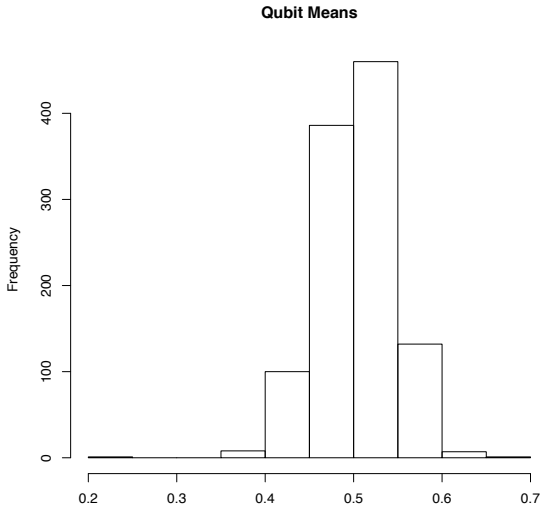


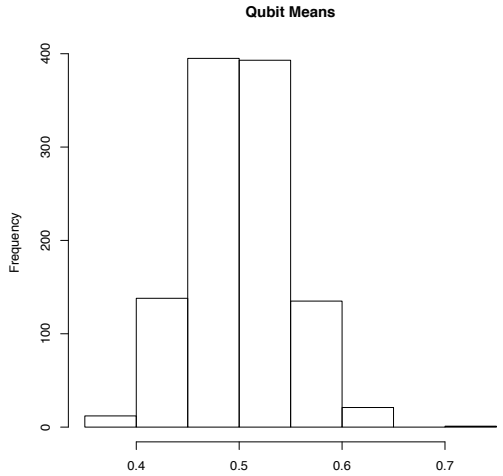


Characterization Results for 1095 Qubits I

- Mean = mean of 8000 samples for each of 1095 qubits
  - Vary from about .35 to .65, with occasional more extreme values







Characterization Results for 1095 Qubits II

- Temporal correlation within qubits
  - Strings of 0s and of 1s are too long for independence to hold
- No apparent spatial correlation in qubit means
- Evidence of negative spatial correlation in qubit values
  - Within-cell neighbors, coupled qubits in different cells, coupled qubits in the same cell

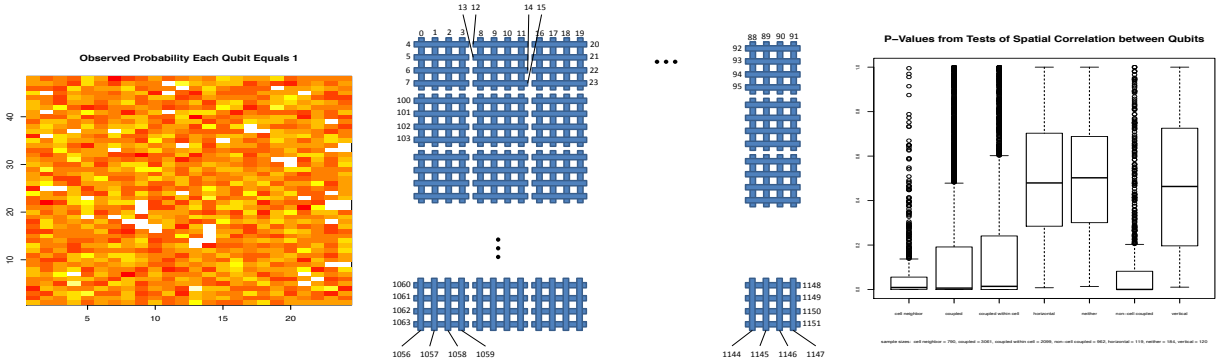


Diagram by Denny Dahl

UNCLASSIFIED

Future Work

- Develop a statistical or other model for the bit string data
  - Requires additional characterization work
- Transform raw bit strings to random bit strings
- Test results using standard RNG tests, e.g., TestU01

Acknowledgements

- Denny Dahl
- Mauricio Reis
- Trevor Lanting
- Bill Press